

REMARKS

The Examiner rejected claim 1 under 35 U.S.C. §103(a) as allegedly being unpatentable over Sherer (U.S. Patent No. 6,115,376) in view of Glawitsch (U.S. Patent No. 6,772,334 B1) and further in view of Frantz (U.S. Patent No. 6,697,943 B1).

The Examiner rejected claims 2-13 and 15-21 under 35 U.S.C. §103(a) as allegedly being unpatentable over Sherer (U.S. Patent No. 6,115,376) in view of Stern (U.S. Patent No. 5,935,249) and further in view of Frantz (U.S. Patent No. 6,697,943 B1).

The Examiner rejected claim 14 under 35 U.S.C. 103(a) as allegedly being unpatentable over Sherer (U.S. Patent No. 6,115,376) in view of Stern (U.S. Patent No. 5,935,249) and further in view of Frantz (U.S. Patent No. 6,697,943 B1) and further in view of Glawitsch (U.S. Patent No. 6,772,334 B1).

Applicants respectfully contend that the Examiner has not provided any argument supporting the rejection of claims 10-12 and 17-19. Applicants respectfully request that the Examiner either provide arguments supporting the rejection of claims 10-12 and 17-19, or else indicate that claims 10-12 and 17-19 are allowable.

Applicants respectfully traverse the §103(a) rejections with the following arguments.

35 U.S.C. §103(a): Claim 1

The Examiner rejected claim 1 under 35 U.S.C. §103(a) as allegedly being unpatentable over Sherer (U.S. Patent No. 6,115,376) in view of Glawitsch (U.S. Patent No. 6,772,334 B1) and further in view of Frantz (U.S. Patent No. 6,697,943 B1).

With regard to claim 1, Applicants respectfully contend that claim 1 is not unpatentable over Sherer in view of Glawitsch and further in view of Frantz, because Sherer in view of Glawitsch and further in view of Frantz does not teach or suggest each and every feature of claim 1.

A first reason why claim 1 is not unpatentable over Sherer in view of Glawitsch and further in view of Frantz is that Sherer in view of Glawitsch and further in view of Frantz does not teach or suggest the feature: "receiving a message by the network-addressable device from a target of a denial of service attack by the spoofing vandal, said attack comprising a denial of service communication sent by the spoofing vandal to the target; [and] detecting, by the network-addressable device, a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative of the denial of service attack on the target by the spoofing vandal using an identity of the network-addressable device in the denial of service communication, said detecting being performed after said receiving has been performed".

Applicants note that in claim 1, the target receives the message before the detecting step is performed, whereas in Glawitsch the target does not receive the message until after the detection step has been performed and until after the detecting step authenticates a request for a session between a client and a server (see Glawitsch, col. 9, lines 65-67; col. 3, lines 32-34). The purpose of Glawitsch's invention is prevent the target from "running out of state" (i.e.,

exhausting resources for communicating with other servers or clients) (see Glawitsch, col. 2, lines 30-47). Glawitsch's invention accomplishes this objective by performing the three-way handshake (SYN, SYN-ACK, ACK) in behalf of the victim before the victim receives the message. Thus, Glawitsch teaches away from the message being received by the target before the detecting step is performed.

Moreover, in claim 1 the network-addressable device performs the detecting step, and the identity of the network-addressable device is used by the vandal to effectuate the communication protocol violation consequent to the message, whereas in Glawitsch a firewall performs the detecting step, and the identity of the firewall is not used by the vandal to effectuate the communication protocol violation consequent to the message.

Also, Sherer does not teach that the vandal is engaged in a denial of service attack on the victim, as acknowledged by the Examiner. Based on the preceding discussion, Glawitsch's method of dealing with a denial of service attack is incompatible with claim 1. Therefore, it is not obvious to modify Sherer by the alleged teaching of Glawitsch.

A second reason why claim 1 is not unpatentable over Sherer in view of Glawitsch and further in view of Frantz is that Sherer in view of Glawitsch and further in view of Frantz does not teach or suggest the feature: "generating, by the network-addressable device, a spoofing alert responsive to the act of detecting the communication protocol violation."

The Examiner argues: "Sherer and Glawitsch, however do not explicitly teach generating a spoofing alert upon detection of protocol violation. Referring to claim 1, Franz teaches generating spoof control packet, setting the alerts and discarding the packets (see abstract and

Fig. 3, blocks 340 and 399). Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to use a system for address authentication having functionality for determining whether the protocol violation is a denial of service attack by the spoofer using address of a network device and generating a spoofing alert as taught in Frantz. One of ordinary skill in the art would have been motivated to use a system for address authentication having functionality for determining whether the protocol violation is a denial of service attack by the spoofer using address of a network device and generating a spoofing alert as taught in Frantz for discarding the packet (see Frantz, Fig.5)."

In response, Applicants acknowledge that Franz teaches discarding the packet. However, Applicants respectfully contend that: (1) discarding the packet is not a spoofing alert; and (2) Franz does not teach or suggest generating a spoofing alert for discarding the packet.

35 U.S.C. §103(a): Claims 2-13 and 15-21

The Examiner rejected claims 2-13 and 15-21 under 35 U.S.C. §103(a) as allegedly being unpatentable over Sherer (U.S. Patent No. 6,115,376) in view of Stern (U.S. Patent No. 5,935,249) and further in view of Frantz (U.S. Patent No. 6,697,943 B1).

Since claims 4-6, 9, 13-14, 16, and 20-21 have been canceled, the rejection of claims 4-6, 9, 13-14, 16, and 20-21 under 35 U.S.C. §103(a) is moot.

Since claims 7-8 have been amended to depend from new claim 22, the rejection of claims 7-8 under 35 U.S.C. §103(a) is moot.

With regard to claim 2, Applicants respectfully contend that claim 2 is not unpatentable over Sherer in view of Stern and further in view of Frantz.

A first reason why claim 2 is not unpatentable over Sherer in view of Stern and further in view of Frantz is that Sherer in view of Stern and further in view of Frantz does not teach or suggest the feature: "receiving a message by the network-addressable device; [and] detecting a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative of activity of a spoofing vandal **using the identity of the network-addressable device in an attack on a target**" (emphasis added).

The Examiner argues: "the limitation "receiving a message by the network-addressable device" is met by a packet (102 in Fig 4.), which is transmitted to interconnection device (100)."

In response, Applicant note that the Examiner has identified the interconnection device 100 of Sherer as allegedly representing the network-addressable device of claim 2. Therefore, antecedent basis considerations in the preceding feature of claim 2 require a disclosure by Sherer

that the communication protocol violation is indicative of activity of a spoofing vandal using the identity of the interconnection device 100 in an attack on a target. Applicants contend that Sherer does not disclose that the communication protocol violation is indicative of activity of a spoofing vandal using the identity of the interconnection device 100 in an attack on a target, as required by claim 2. The Examiner's argument has not even addressed the issue of whether Sherer discloses "using the identity of the network-addressable device in an attack on a target". Therefore, claim 2 is not unpatentable over Sherer in view of Stern and further in view of Frantz.

A second reason why claim 2 is not unpatentable over Sherer in view of Stern and further in view of Frantz is that Sherer in view of Stern and further in view of Frantz does not teach or suggest the feature: "advancing the value of a counter associated with the target". Although the Examiner alleges that Stern teaches a counter for storing a counter value, the Examiner does not allege that Stern teaches "advancing the counter" as required by claim 2. Indeed, rather than teaching "advancing the counter", Stern teaches the very opposite, namely "decrementing" the counter. See Stern, col. 16, line 36. Therefore, claim 2 is not unpatentable over Sherer in view of Stern and further in view of Frantz.

A third reason why claim 2 is not unpatentable over Sherer in view of Stern and further in view of Frantz is that Sherer in view of Stern and further in view of Frantz does not teach or suggest the feature: "generating a spoofing alert when the value of the counter exceeds the threshold". Indeed, none of the references cited by the Examiner teach the preceding feature of claim 2. Therefore, claim 2 is not unpatentable over Sherer in view of Stern and further in view

of Frantz.

A fourth reason why claim 2 is not unpatentable over Sherer in view of Stern and further in view of Frantz is that the Examiner's arguments for modifying Sherer by the alleged teaching of Stern and Franz is not persuasive.

The Examiner argues: "Therefore at the time the invention was made, it would have been obvious to one of ordinary skill in the art, to modify a system for access control address authentication of Sherer by using the counter and comparing the value of the counter with the threshold as taught in Stern and generating a spoofing alert as taught in Frantz. One of ordinary skill in the art would have been motivated to modify a system for access control address authentication by using the counter and comparing the value of the counter with the threshold as taught in Stern for issuing the authorization command (see Stern column 16, lines 39-40) and **generating a spoofing alert as taught in Frantz for discarding the packet** (see Frantz, Fig.5)" (emphasis added).

In response, Applicant respectfully contend that the Examiner's suggested modification of Sherer (i.e., "using the counter and comparing the value of the counter with the threshold ") does no more than provide alleged advantages to Sherer's invention which already exists in Sherer's invention without a counter. The advantages allegedly promoted by the modification of Sherer include "generating a spoofing alert" and "discarding the packet". However, Sherer discloses in col. 6, lines 37-45: "If the MAC address is not authorized, then **the packet is blocked**, and the port is disabled or other action is taken to prevent that end station from accessing the layer two fabric of the network. Further, a **notification message can be sent to a**

09/849,697

14

network management station, indicating that a failed authentication occurred" (emphasis added). Thus, Sherer does not have any use for the counter because Sherer already discloses (without need of a counter): blocking the packet and sending a notification message to a network management station. Therefore, modifying Sherer by adding a counter to Sherer's invention adds unnecessary complexity and unnecessary processing time to Sherer's invention.

In other words, the Examiner's suggested modification of Sherer degrades the performance of Sherer's method without adding anything of value to Sherer's method. Accordingly, Applicant respectfully contend that the Examiner has not established a *prima facie* case of obviousness in relation to claim 2. Therefore, claim 2 is not unpatentable over Sherer in view of Stern and further in view of Frantz.

Based on the preceding arguments, Applicants respectfully maintain that claim 2 is not unpatentable over Sherer in view of Stern and further in view of Frantz, and that claim 2 is in condition for allowance. Since claims 3, 10-12, 15, and 17-19 depend from claim 2, Applicants respectfully contend that claims 3, 10-12, 15, and 17-19 are likewise in condition for allowance.

In addition, Applicants respectfully contend that the Examiner has not provided any argument supporting the rejection of claims 10-12 and 17-19. Accordingly, the Examiner has not established a *prima facie* case of obviousness in relation to claims 10-12 and 17-19. Applicants respectfully request that the Examiner either provide arguments supporting the rejection of claims 10-12 and 17-19, or else indicate that claims 10-12 and 17-19 are allowable.

CONCLUSION

Based on the preceding arguments, Applicants respectfully believe that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicants invites the Examiner to contact Applicants' representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account 09-0457.

Date: 06/29/2005

Schmeiser, Olsen & Watts
3 Lear Jet Lane, Suite 201
Latham, New York 12110
(518) 220-1850

Jack P. Friedman
Jack P. Friedman
Registration No. 44,688